UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In the Matter of the Search of:	)	
	)	**Case No:** 2:24-mj-452
Information, including the content of communications,	)	
associated with the Google emails listed	)	**Magistrate Judge:** Deavers
in Attachment A and collectively referred to as	)	
SUBJECT ACCOUNTS, that are stored at the	)	
premises Controlled by Google LLC	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew W. Guinn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a SA with the FBI and have been since April 2012. I am currently assigned to the Child Exploitation and Human Trafficking Task Force Crimes Against Children Squad, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses involving children. As part of my duties as a SA, I investigate criminal violations relating to child exploitation and child pornography, including the online enticement of minors and the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with the following Google accounts:

   1.Tobioyedokun9@gmail.com
   2.Oladimeji12340@gmail.com
   3.yourshortgurl@gmail.com

   (collectively the **SUBJECT ACCOUNTS**) that are stored at premises controlled by Google, a Google of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNTS.**

5. The **SUBJECT ACCOUNTS** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor, possession of child pornography, as well as 18 USC § 875(d) – extortion via interstate communications. I am requesting authority to search the **SUBJECT ACCOUNTS**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

6. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the production, distribution, transmission, receipt, and/or possession of child

pornography and the coercion and enticement of a minor, as well as 18 USC §875(d) – extortion via interstate communications extortion via interstate communications are presently located in the **SUBJECT ACCOUNTS.** I have not omitted any facts that would negate probable cause.

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child

pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. Title 18, United States Code, Section 875, makes it a federal crime for any person to, with the intent to extort from another person, firm, association, or corporation, any money or thing of value, to transmit in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee of another.

11. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

12. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined pursuant to Title 18, United States Code, Section 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

13. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

14. The term "minor," as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
15. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.
16. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
17. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
18. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
19. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through

networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

20. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

21. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

BACKGROUND INFORMATION REGARDING GOOGLE, GMAIL AND TECHNOLOGY

22. Google, LLC provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage.

23. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone

number, and, in some cases, a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.

24. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.

25. Notably, Google, LLC also provides "cloud" storage services. Account holder/users can utilize this service, which is called "Google Drive," to store pictures, videos, and other electronic files remotely and without taking up memory space on their personal computer, smart phone, and physical storage media.

26. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

27. These services may include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

28. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers.
29. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.
30. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.
31. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop

or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI").

32. Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.

33. In addition, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common 7 computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.

34. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

35. In summary, based on my training and experience in this context, I believe that the servers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers), as well as Google-generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

36. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to

commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INVESTIGATION AND PROBABLE CAUSE

37. On May 22, 2024, the FBI received an online tip from Jane Doe One regarding her son, Minor Victim One (MV1), date of birth 08/XX/2009. The tip stated that MV1 had been a victim in a sextortion scam. Jane Doe One noted that an unknown subject sent a text to MV1 containing an explicit and inappropriate photo of a girl and then requested a picture of MV1's "private parts," then began to threaten exposure if MV1 did not send money to the unknown subject. Jane Doe One further stated that extortionist used the phone number (972) 977-2851 and the email address Tobioyedokun9@gmail.com in their demands of MV1.

38. On May 24, 2024, an interview was conducted with Jane Doe One, during which she stated the Instagram account that was used to extort MV1was "ca_ssie800" with the name "Cassie."

39. Some of the chat messages between MV1 and the unknown **SUBJECT ACCOUNT** "Cassie" were obtained by law enforcement. In those messages, "Cassie" asked MV1 if MV1 wanted to "get freaky," to which MV1 asked "Cassie" to start. "Cassie" then requested a photo of MV1 to get her "wet." MV1 and "Cassie" messaged back and forth about who would send the first photo, at which point, "Cassie" distributed to MV1 an image of a vagina. MV1 and "Cassie" then appeared to get on a video call. After the call, "Cassie" sent MV1 one photograph of MV1 taking a selfie with face visible, one photograph of a penis, one photograph of an Instagram page, and one photograph of a telephone number.

40. "Cassie" then sent a message to MV1 which stated "I'm gonna send this pics to all your school pages Facebook and Instagram and all the pages in the city it both indicate live cam it gonna go viral so soon and to all your family and friends. You can stop talking and bluff then i will immediately, you just an option tho…I'm gonna send it to all your friends and family on insta right now." MV1 asked "if she was joking" and "Cassie" responded "Do you think I'm joking…Pay me 200."

41. Hundreds of other messages were exchanged and, in summary, those messages revealed "Cassie" demanded money from MV1 and continued to threaten him that if he did not,

she would make sure MV1's photograph of his penis went "viral." Ultimately, MV1 transferred $50.00 via Amazon.

42. On June 12, 2024, your affiant served a subpoena on Meta Platforms requesting subscriber records and IP tolls for the following: Instagram account username "ca_ssie800" and telephone number (972) 977-2851 as well as email address Tobioyedokun9@gmail.com. In response, Meta Platforms provided responsive records that stated there were no records related to the telephone number. Meta did provide the following information about the "cassie800" Instagram account:

First Name:	Cassie
Vanity Name:	ca_ssie800
Registration Date:	2023-05-30 17:12:05 UTC
Registration Ip:	2600:1009:b03b:7949:a112:5a96:3c9d:cb06
Phone Numbers:	+2348072771368 Verified
Logins:	IP Address: 102.88.69.65
	Time: 2024-05-24 22:29:44 UTC
	IP Address: 102.89.22.126
	Time: 2024-05-19 21:00:43 UTC
	IP Address: 102.89.23.40
	Time: 2024-05-19 20:59:48 UTC
	IP Address: 92.119.177.59
	Time: 2024-05-18 23:43:58 UTC

Meta also provided the following information about the Tobioyedokun9@gmail.com:

Account Type:	InstagramUser
Name: First:	Drew Cowther
Registered Email:	tobioyedokun9@gmail.com (Verified)
Vanity Name:	raven_cowther09
Registration Date:	2017-11-27 13:13:55 UTC
Registration IP:	96.39.217.161

43. Also on June 12, 2024, your affiant served a subpoena on AT&T requesting customer and subscriber records for telephone number (972) 977-2851, the number provided by Jane Doe One used to extort MV1. In response, AT&T provided the following information:

FINANCIAL LIABLE PARTY:

Name:	MARY JOLLEY
Credit Address:	514 JEFFERSON LN, LAKE DALLAS, TX 75065
Customer Since:	05/19/2024
Contact Home Email:	TOBIOYEDOKUN9@GMAIL.COM

USER INFORMATION:

MSISDN:	(972) 977-2851
IMSI:	310280121693406
MSISDN	Active: 05/19/2024 - Current
Name:	MARY JOLLEY
User Address:	514 JEFFERSON LN, LAKE DALLAS, TX 75065
Service Start Date:	05/19/2024
Contact Home Email:	TOBIOYEDOKUN9@GMAIL.COM

44. Additionally, on June 12, 2024, your affiant served a subpoena on Google requesting subscriber records for email address tobioyedokun99@gmail.com, the email provided by Jane Doe One used to extort MV1. In response, Google provided the following information:

Google Account ID:	213883993223
Name:	Tobi Oye
Given Name:	Tobi
Family Name:	Oye
E-Mail:	tobioyedokun99@gmail.com
Created On:	2023-02-16 20:42:21 Z
Terms of Service IP:	197.211.59.126
Last Updated Date:	2024-04-17 05:23:10 Z
Recovery SMS:	+2349152274351 [NG]

45. On June 13, 2024, Jane Doe One emailed your affiant a screen-recording of the conversation MV1 had with the unknown target. Your affiant reviewed the recording which confirmed that MV1 was tricked into exposing his penis and then extorted with threats that he would need to pay the unknown target money, or the target would expose the penis of MV1 to family and friends. To facilitate payment, the extortionist provided MV1 with the email addresses which included Oladimeji12340@gmail.com, plqkbxsqzdic@hotmail.com, ocbt642252@hotmail.com, and Tobioyedokun9@gmail.com.

46. On June 13, 2024, your affiant also completed open-source research that linked the email address Tobioyedokun9@gmail.com to an Apple account. Consequently, on or about June 17, 2024, your affiant served a subpoena on Apple requesting subscriber and customer records for tobioyedokun9@gmail.com. In response, Apple provided the following information:

Person ID: 20326850824

signup_ts: 2021-07-29 20:36:48
email_addr_txt: tobioyedokun9@gmail.com, yourshortgurl@gmail.com
last_name: Oyedokun
fist_name: Tobi
Address: 4966 SE 149th ST, Summerfield, FL 34491
Phone: 352-693-9926

47. On or about June 17, 2024, your affiant served a subpoena on PayPal requesting customer information for: plqkbxsqzdic@hotmail.com (an email address provided by the SUBJECT to MV1). In response, PayPal provided the following customer records which included four unsuccessful payment attempts from MV1 to the account holder on May 22, 2024, in amount of $44.14 for each transaction.

48. On June 17, 2024, your affiant served a subpoena on Google requesting subscriber records for email address Oladimeji12340@gmail.com, an email provided by the SUBJECT. In response, Google provided the following:

Google Account ID: 815441643325
Name: Ola Dimeji
Given Name: Ola
Family Name: Dimeji
e-Mail: oladimeji12340@gmail.com
Created on: 2021-07-20 03:41:21 Z
Terms of Service IP: 129.205.124.218
Login: 2024-05-29 19:33:14 Z
Recovery SMS: +2349024624459 [NG]

49. On or about June 28, 2024, your affiant served a subpoena on Google requesting subscriber records for email address yourshortgurl@gmail.com, an email provided by Apple (see paragraph 31). In response, Google provided the following:

Google Account ID: 92350022379
Name: Your Shortgurl
Given Name: Your
Family Name: Shortgurl
e-Mail: yourshortgurl@gmail.com
Created on: 2024-05-10 09:27:19 Z
Terms of Service IP: 102.89.46.58
IP ACTIVITY

Timestamp	IP Address	Activity Type
2024-05-29 19:33:14 Z	102.89.41.138	Login
2024-05-19 22:41:56 Z	102.89.22.126	Login
2024-05-10 09:27:21 Z	102.89.46.58	Login

50. Based on the information that has been gathered to date by your affiant, including

interviews with the identified victim's mother noted above, law enforcement reports, subpoena requests and returns, and social media exchanges including, but not limited to, those taking place on Instagram, your affiant has reason to believe that the individual utilizing the **SUBJECT ACCOUNTS,** most likely an individual residing overseas, was threatening MV1 in a bid to obtain nude or sexually explicit images and videos of them while also using child pornography images already obtained in order to gather more exploitation material. Therefore, it is likely that the **SUBJECT ACCOUNTS** contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications.

COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

51. Based on my own knowledge, experience, and training in online child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in minors and/or seek to sexually exploit minors via online communications:

    A. Those who have a sexual interest in minors, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from discussions of or literature describing such activity.

    B. Those who have a sexual interest in children and/or seek to sexually exploit minors via online communications may collect sexually explicit or suggestive materials in a variety of media. These materials are frequently used for the sexual arousal and gratification of the individual. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

    C. Individuals who have a sexual interest in children have been found to: download, view, then delete child pornography on a cyclical and repetitive

basis; view child pornography without downloading or saving it; or save child pornography materials to cloud storage.

D. Those who have a sexual interest in minors may correspond online with and/or meet others to share information about how to find child victims, exchange stories about their sexual exploits with children, and/or exchange child pornography materials; and tend to conceal and maintain in a safe, secure and private environment such correspondence as they do any sexually explicit material related to their illicit sexual interest.

E. When communications relating to a sexual interest in children, and/or child pornography files are stored on or accessed by computers and related digital media, forensic evidence of the accessing, downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such files have been deleted from the computers or digital media.

52. Based upon the conduct of individuals who have a sexual interest in children and/or seek to sexually exploit, coerce, or entice minors via online communications, as set forth in the above paragraphs, there is probable cause to believe that evidence of the violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications. is currently located on the **SUBJECT ACCOUNTS.**

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

53. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(1)(A), by using the warrant to require Google LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

CONCLUSION

54. Based on the forgoing factual information, your affiant submits there is probable cause to

believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications, and evidence of those violations is located in the content of the **SUBJECT ACCOUNTS**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** described in Attachment A, and the seizure of the items described in Attachment B.

55. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Google who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Matthew W. Guinn
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me 10th day of September, 2024.

Elizabeth A. Preston Deavers
United States Magistrate Judge